VODIČ:

CENTAR ZA PREVENCIJU BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA - CERT

SHARE FONDACIJA

Organizacija za evropsku bezbednost i saradnju
Misija u Srbiji

Шведска
Sverige

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

Република Србија
Министарство трговине, туризма и телекомуникација

VODIČ:

CENTAR ZA PREVENCIJU BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA - CERT

VODIČ: CENTAR ZA PREVENCIJU BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA - CERT
SHARE FONDACIJA
DECEMBAR 2019.
UREDNICI: ANDREJ PETROVSKI, ALEKSANDRA RISTIĆ
AUTORI: DANILO KRIVOKAPIĆ, ANDREJ PETROVSKI, BOJAN PERKOV,
SONJA KOLUNDŽIJA, MAJA LAKUŠIĆ
OBRADA TEKSTA: BOJAN PERKOV
DIZAJN I PRELOM: OLIVIA SOLIS VILLAVERDE

ŠTAMPARIJA: BEOPRINT
TIRAŽ: 1000

Publikacija je izrađena uz finansijsku podršku Švedske agencije za međunarodnu razvojnu saradnju, u okviru projekta Konsolidovanje procesa demokratizacije u sektoru bezbednosti u Republici Srbiji.

SADRŽAJ

PREDGOVOR

PREDGOVOR

Regulatorna agencija za eletronske komunikacije i poštanske usluge (RATEL) je 2016. godine, Zakonom o informacionoj bezbednosti, prepoznata kao jedan od najznačajnijih subjekata u oblasti informacione bezbednosti, pa je ovim Zakonom dobila u nadležnost i obavljanje poslova Nacionalnog CERT-a. Zahvaljujući sveukupnom kvalitetu rada naše Agencije u polju regulacije tržišta telekomunikacija i poštnaskih usluga utvrđena je ova izuzetno značajna, odgovorna i prestižna uloga ključnog činioca u oblasti informacione bezbednosti u Republici Srbiji. Iste godine utvrđen je plan za stručno usavršavanje i osposobljavanje zaposlenih, koje je izuzetno važno u ovoj dinamičnoj oblasti, i tokom 2017. godine formiran tim Nacionalnog CERT-a. Upravo iz tog razloga, formiran je mlad tim, spreman na predan i odgovovoran rad, svestan neophodnosti stalnog usavršavanja. Naš cilj bio je kvalitet u radu koji podrazumeva i sam naziv Nacionalnog CERT-a, pa je bilo potrebno određeno vreme kako bi se dostigao planirani nivo znanja i sposobnosti. Smatramo da je obim, ali i nivo, obavljenih poslova iz delokruga nadležnosti Nacionalnog CERT-a postao najvidljiviji tokom ove godine. U oblasti promocije značaja informacione bezbednosti temeljno su planirane aktivnosti za sve tri ciljne grupe – građane, privredne subjekte i organe vlasti. Treba naglasiti i da su sve aktivnosti utvrđene Akcionim planom za sprovođenje Strategije razvoja informacione bezbednosti sprovedene u propisanim rokovima. Stupanjem na snagu izmena i dopuna Zakona o informacionoj bezbednosti ojačan je položaj Nacionalnog CERT-a i prepoznata ideja rukovodstva Agencije od samog dobijanja nadležnosti Nacionalnog CERT-a kroz obezbeđivanje stručnog kadra i opremljenosti odgovarajućim sistemima za obavljanje poslova iz delokruga nadležnosti.

Naša država primenila je jedan od modela organizacije CERT-ova koji podrazumeva uspostavljanje Nacionalnog CERT-a kao jedinstvene kontakt tačke za koordinaciju incidenata, čiji tim za tehničku podršku zapravo predstavljaju svi posebni CERT-ovi, a čije angažovanje u slučaju incidenta zavisi od oblasti poslovanja. Tokom ove godine upisana su tri posebna CERT-a, te je trenutno u evidenciju upisano devet posebnih CERT-ova. Smatramo da je veoma važno da kompanije koje se bave informacionom bezbednošću prepoznaju prednosti i značaj upisa u evidenciju posebnih CERT-ova, koji zapravo predstavlja jedan od dokaza kvaliteta njihovog rada. Sa druge strane, važno je da građani, privredni subjeki i organi vlasti budu svesni izazova koje nosi informaciona bezbednost i da kroz podizanje svesti utičemo na prevencijurizika koji postoje.

dr Vladica Tintor, direktor Regulatorne agencije za eletronske komunikacije i poštanske usluge Republike Srbije (RATEL)

ŠTA JE TO CERT?

ŠTA JE TO CERT?

Centri za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima su organizacije posvećene zaštiti informacione bezbednosti (eng. Computer Emergency Response Team, CERT), i mogu biti uspostavljeni na nacionalnom nivou, na nivou sektora (kao što su finansije ili energetika) kao i u okviru jednog pravnog subjekta. Alternativno, ove organizacije se zovu CSIRT (Computer Security Incident Response Team) ili CIRT (Computer Incident Response Team).

U zavisnosti od pravnog okvira, uloga CERT-a može biti edukativna, savetodavna, preventivna i istraživačka, što između ostalog podrazumeva praćenje incidenata na nacionalnom nivou, pružanje ranih upozorenja i informacija o rizicima i incidentima u oblasti informacione bezbednosti, ali i promociju bezbednosne kulture među građanima, u državnim institucijama i privatnom sektoru. Posebni CERT-ovi, usled činjenice da su zaduženi za ograničen broj konkretnih informacionih sistema, najčešće imaju funkciju upravljanja incidentima, što podrazumeva aktivniju ulogu u procesu ponovnog uspostavljanja normalnog funkcionisanja sistema, analizu incidenta i eventualnog malicioznog softvera.

Prvom organizacijom ove vrste smatra se CERT koordinacioni centar (CERT/CC) Instituta za softverski inženjering na Karnegi Melon univerzitetu u Pitsburgu, SAD. CERT/CC je osnovan 1988. godine, nakon incidenta sa tzv. Moris crvom, jednim od prvih kompjuterskih virusa distribuiranih preko interneta. Virus je onesposobio na hiljade povezanih kompjutera, razotkrivajući ranjivost mreže. Razvoj interneta od tada podrazumeva sve bolju zaštitu, ali se istovremeno unapređuju i tehnike za narušavanje bezbednosti mreže. Tako je CERT/CC postao deo CERT odeljenja Instituta za softverski inženjering, čija su dodatna polja delovanja edukacija i sprovođenje treninga, istraživanje i razvoj, podizanje svesti, forenzika, organizaciona bezbednost i uspostavljanje globalnih odnosa.[1]

Već 1990. godine nacionalne organizacije su osnovale međunarodnu organizaciju FIRST (Forum of Incident Response and Security Teams)[2] koja trenutno broji više od 400 članova širom sveta. FIRST okuplja CERT timove na drzavnom nivou, komercijalne CERT-ove i CERT-ove akademske zajednice.

1 Istorijat CERT/CC, dostupno na: sei.cmu.edu
2 O Forumu: first.org

CERT U NACIONALNOM ZAKONODAVSTVU

CERT U NACIONALNOM ZAKONODAVSTVU

Zakon o informacionoj bezbednosti ("Službeni glasnik RS", broj 6/16, 94/17 i 77/19, u daljem tekstu: ZIB) stupio je na snagu u februaru 2016. godine, dok su izmene i dopune izvršene tokom 2017. i 2019. godine.

Ovim zakonom propisane su 4 vrste CERTova i njihove nadležnosti:

- Nacionalni CERT;
- CERT organa vlasti;
- CERT samostalnih operatora IKT sistema;
- Poseban CERT.

Iako ZIB koristi englesku skraćenicu CERT, ona ne predstavlja pravi akronim u našem pravnom sistemu, zakonodavac se odlučio da zadrži međunarodno prihvaćenu skraćenicu, dobro poznatu među stručnjacima za informacionu bezbednost, kako bi se izbegla konfuzija stvaranjem novih akronima ili upotrebom predugih naziva.

ŠTA JE NACIONALNI CERT?

Nacionalni CERT je organizacija koje obavlja poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima u Republici Srbiji na nacionalnom nivou. Nacionalni CERT je ekspertska organizacija čija je glavna nadležnost koordinacija i komunikacija na nacionalnom i međunarodnom nivou, u cilju prevenicije i upravljanja bezbednosnim rizicima.

Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima Republike Srbije osnovan je u okviru Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL), u skladu sa Zakonom o informacionoj bezbednosti.

Primarna zaduženja Nacionalnog CERT-a su koordinacija prevencije i zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima (IKT sistemima) na nacionalnom nivou. Nacionalni CERT prikuplja i razmenjuje informacije o mogućim rizicima, a zatim obaveštava, upozorava i savetuje lica koja upravljaju IKT sistemima, kao i javnost Republike Srbije.

Nacionalni CERT prati prijavljene incidente na nacionalnom nivou i na osnovu prikupljenih podataka analizira rizike i incidente sa ciljem podizanja svesti o značaju informacione bezbednosti građana, privrednih subjekata i organa javne vlasti.[3]

Nacionalni CERT vodi evidenciju posebnih CERT-ova.

ŠTA JE CERT ORGANA VLASTI?

CERT organa vlasti obavlja poslove koji se odnose na zaštitu od incidenata u IKT sistemima organa vlasti. Poslovi CERT-a organa vlasti obuhvataju zaštitu jedinstvene informaciono-komunikacione mreže elektronske uprave, koordinaciju i saradnju sa operatorima IKT sistema koje povezuje jedinstvena mreža, u prevenciji incidenata, otkrivanju incidenata, prikupljanju informacija o incidentima i otklanjanju posledica incidenata, kao i izdavanje stručnih preporuka za zaštitu IKT sistema za rad sa tajnim podacima. Za obavljanje poslova CERT-a organa vlasti nadležna je Kancelarija za IT i eUpravu.

3 O Nacionalnom CERT-u, dostupno na: cert.rs

ŠTA JE CERT SAMOSTALNIH OPERATORA IKT SISTEMA?

Samostalni operatori IKT sistema (ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove i službe bezbednosti) su u obavezi da formiraju sopstvene CERT-ove radi upravljanja incidentima u svojim sistemima. Samostalni CERT-ovi međusobno razmenjuju informacije o incidentima, kao i sa Nacionalnim CERT-om i CERT-om organa vlasti, a po potrebi i sa drugim organizacijama. Pored ovih poslova samostalni CERT-ovi obavljaju i izradu internih akata u oblasti informacione bezbednosti, izbor, testiranje i implementaciju mera zaštite od kompromitujućeg elektromagnetnog zračenja, nadzor implementacije i primene bezbednosnih procedura, upravljanje i korišćenje kriptografskih proizvoda, analizu bezbednosti IKT sistema u cilju procene rizika, kao i obuku zaposlenih u oblasti informacione bezbednosti.

ŠTA JE POSEBAN CERT?

Posebni CERT-ovi obavljaju poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima. Njihova specifičnost se ogleda u tome što su specijalizovani za određenu oblast ili grupu pravnih subjekata kao što su, na primer, različite grane privrede, finansijske institucije, državni organi, civilni sektor, akademski sistem i slično, te stoga prate stanje i reaguju u slučaju incidenata samo u toj oblasti ili grupi. Posebni CERT je pravno lice ili organizaciona jedinica pravnog lica sa sedištem na teritoriji Republike Srbije koje obavlja poslove iz oblasti informacione bezbednosti, čiji zaposleni poseduju stručna i tehnička znanja i spremni su da pruže specijalizovanu podršku svojim korisnicima.

U skladu sa Zakonom, poseban CERT može biti pravno lice ili organizaciona jedinica u okviru pravnog lica. Ovaj status se formalno stiče upisom u evidenciju posebnih CERT-ova na osnovu prijave Nacionalnom CERT-u, odnosno RATEL-u. Sam postupak registracije je regulisan Pravilnikom o bližim uslovima za upis u evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima (“Službeni glasnik RS”, broj 12/17).

SHARE CERT je prvi poseban CERT registrovan u Republici Srbiji u skladu sa Zakonom, 3. aprila 2017. godine. Specijalizovan za pružanje pravne i tehničke podrške onlajn i građanskim medijima u Srbiji koji su pretrpeli tehničke napade, SHARE CERT je formiran na osnovu iskustva stručnog tima SHARE Fondacije u pružanju ovakve vrste podrške u više od stotinu slučajeva proteklih godina. Tim SHARE CERT-a godinama se aktivno bavi istraživanjem i sistematizacijom znanja iz oblasti informacione bezbednosti onlajn i građanskih medija, publikovanjem priručnika, organizovanjem javnih diskusija u saradnji sa nadležnim državnim institucijama, kompanijama i organizacijama civilnog društva, kao i treninga i radionica na temu informacione bezbednosti u Srbiji i inostranstvu.[4]

Organizacija, dakle, može obavljati poslove posebnog CERT-a i pre formalne registracije, međutim, upis u registar pruža dodatnu vidljivost, olakšava korisnicima kontakt sa posebnim CERT-om i unapređuje saradnju posebnog i Nacionalnog CERT-a, kao i između posebnih CERT-ova. Konačno, upis u registar istovremeno predstavlja potvrdu o ispunjavanju propisanih uslova, svojevrsnu sertifikaciju da je organizacija sposobna da obavlja poslove CERT-a.

Do zaključenja ove publikacije u evidenciju posebnih centara za prevenciju bez-

bednosnih rizika u IKT sistemima upisano je devet posebnih CERT-ova.[5]

ZNAČAJ SARADNJE

Komunikacija različitih CERT-ova unapređuje operativnu bezbednost u tehničkom smislu, ali i razvoj poverenja među akterima, što je od naročitog značaja kada je reč o saradnji Nacionalnog i posebnih CERT-ova. Redovna komunikacija neophodna je akterima za optimizaciju kapaciteta, dok blagovremena razmena informacija istovremeno omogućava efikasne reakcije u slučaju incidenta.

Jedna od Zakonom definisanih uloga Nacionalnog CERT-a jeste vođenje evidencije posebnih CERT-ova, na koji način Nacionalni CERT razvija saradnju javnog i privatnog sektora. Budući da su posebni CERT-ovi, pored razvoja u svojoj oblasti, dužni da grade kapacitete za saradnju sa postojećim CERT-ovima, Nacionalni CERT je koordinator informacija o incidentima na nacionalnom nivou, ali obavlja i poslove prikupljanja i usmeravanja informacija, znanja i dobre prakse među različitim akterima.

Kontinuirana saradnja CERT-ova, bez obzira na to da li su javni ili privatni, treba da se odvija na tehničkom i stručnom nivou. Osim na principu deljenja resursa između CERT-ova koji imaju različite kapacitete i polja stručnosti, njihova saradnja se zasniva i na razmeni znanja, relevantnih i aktuelnih informacija i iskustava. Bez obzira da li će i kako u daljoj primeni novih zakonskih rešenja države svojim resursima pomagati formiranje posebnih CERT-ova kako bi se pokrila svaka oblast sistema, javno-privatno partnerstvo može poslužiti kao dobar mehanizam, posebno na nivou tehničke i stručne saradnje u pravcu racionalizacije resursa.

Imajući u vidu da je za održavanje adekvatnog nivoa informacione bezbednosti u Republici Srbiji neophodno uključivanje svih relevantnih činilaca, javno-privatno partnerstvo je definisano kao strateški cilj Republike Srbije, a u okviru prioritetne oblasti uspostavljanja i jačanja saradnje među svim relevantnih subjektima u oblasti informacione bezbednosti.

Poslednjim izmenama Zakona o informacionoj bezbednosti predviđeno je da je održavanje kontinuirane saradnje među svim CERT organizacijama u nadležnosti Nacionalnog CERT-a, koji će organizovati međusobne sastanke najmanje tri puta godišnje.

Zakonom o informacionoj bezbednosti ostavljen je prostor za uključivanje aktera iz privatnog, akademskog i civilnog sektora u napore usmrene na jačanje infrmacione bezbednosti putem formiranja posebnih radnih grupa. U tom smislu saradnja privatnog i javnog sektora treba da omogući efikasnu komunikaciju i optimizaciju planiranih budućih aktivnosti, odnosno blagovremenu razmenu informacija i deljenje resursa.

Saradnja između javnog i privatnog sektora može da bude veoma značajna za industrijska istraživanja i inovacije u oblasti informacione bezbednosti, a veoma bitan segment saradnje je razmena informacija u cilju adekvatne pripremljenosti i odgovora na bezbednosne rizike i incidente.[6]

U slučaju sajber incidenta na nacionalnom nivou, posebni CERT-ovi imaju važnu ulogu u reagovanju na incident, rešavanju incidenta i saniranju posledica incidenta, upravo zbog činjenice da su to zapravo najstručnije, odnosno najkompetetnije kompanije u našoj zemlji koje imaju jasno utvrđen katalog usluga u oblasti zaštite od bezbednosnih rizika i incidenata u IKT sistemima.

5 Evidencija posebnih CERT-ova dostupna je na: cert.rs

6 Vlada Republike Srbije, Strategija razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine, 2017. Dostupno na: ratel.rs

OSNOVNI PROCESI U RADU CERT-A

OSNOVNI PROCESI U RADU CERT-A

Zadatak svakog CERT-a je da prati i analizira pretnje po bezbednost IKT sistema, pruža pomoć u prepoznavanju pretnji i prevenciji napada, osnažuje aktere za adekvatne odgovore na napad, obezbeđuje pravnu pomoć u procesuiranju sajber incidenata, održava komunikaciju sa nadležnim institucijama i drugo.

Da bi CERT mogao uspešno da realizuje svoje aktivnosti neophodno je da utvrdi katalog usluga, koji je kod Nacionalnih CERT-ova po pravilu definisan zakonom. Ukoliko su usluge, vizija, misija i ciljevi jasno i precizno utvrđeni, uspostavljen je osnovni okvir poslovanja i razvoja CERT-a. To su po pravilu, između ostalog, koordinacija informacija, monitoring sistema za otkrivanje upada, analiza potencijalnih pretnji i napada na bezbednost IKT sistema, oporavak sistema od posledica napada.

Osnovne usluge CERT-ova podrazumevaju predlog i primenu mera zaštite, izveštavanje, analizu i tehničku podršku. One se detaljnije mogu opisati u svetlu svoja četiri osnovna procesa: trijaža, razrešavanje, izdavanje obaveštenja i davanje povratnih informacija korisnicima. Svaki od ovih procesa je potrebno interno dokumentovati, u okviru CERT organizacije, u vidu jasnih opisa.[7]

- Proces trijaže predstavlja osnovnu tačku kontakta i podrazumeva prihvatanje, prikupljanje, sortiranje i prosleđivanje dobijenih informacija. Kada deo CERT tima koji se bavi trijažom dobije neku informaciju ili prijavu problema, šalje se potvrda pošiljaocu da je poruka primljena, a zatim se informacija sortira, prioritizuje, dodaje joj se jedinstveni idenitifikator i prosleđuje se drugim procesima u okviru implementiranih servisa.[8]
- Proces razrešavanja incidenata podrazumeva analizu prijavljenih bezbednosnih incidenata ili pretnji i davanje odgovora na njih. Tokom analize se utvrđuje uzrok, analiziraju se dokazni materijali, utvrđuje se ko je uključen u incident, kao i koja vrsta podrške i u kojoj meri je potrebna. Kakav će odgovor biti zavisi od CERT-ovih misija, ciljeva i definicija usluga, ali i od postavljenih prioriteta.
- Proces izdavanja obaveštenja predstavlja obaveštavanje u različitim formatima, kao što su:

1. najave
2. upozorenja
3. saveti
4. kratka obaveštenja
5. smernice
6. tehničke procedure

Osnovna svrha izdavanja obaveštenja je prosleđivanje informacije korisnicima koje će im pomoći u zaštiti njihovih sistema ili da bi se pronašli tragovi potencijalnog napada davanjem informacija o mogućim, tekućim ili nedavnim pretnjama. Dodatno, sugerišu se metode za prevenciju, otkrivanje ili oporavak od incidenata. Prilikom obaveštavanja korisnika o napadima određenog tipa, treba voditi računa da je nivo informacija koje se otkrivaju dovoljan da korisnici razumeju prirodu napada i mogu da provere da li su postali žrtve tog napada, ali ne toliko detaljne da bi mogle da se upotrebe kao uputstvo za sprovođenje napada.[9]

7 Univerzitet u Beogradu – Elektrotehnički fakultet, Studija izvodljivosti izgradnje Nacionalnog CERT-a, 2016. Dostupno na: ratel.rs
8 Ibid.
9 Ibid.

- Proces davanja povratnih informacija predstavlja komunikaciju sa korisnicima i entitetima, bilo na zahtev ili u regularnoj formi (npr. u formi izveštaja).

Proces upravljanja informacijama obuhvata sve 4 pomenute faze i veoma je važan deo osnovnog procesa. Informacije je potrebno prikupljati i evidentirati, nakon toga verifikovati, kategorizovati i na kraju čuvati. Neke informacije se mogu i objaviti, kako bi se dale smernice ili podrška zainteresovanim stranama, ali tokom čitavog procesa bezbednost svih informacija u okviru CERT organizacije mora biti na najvišem nivou.

Dodatno, proces saradnje podrazumeva sve vrste interakcija koje CERT ima sa drugim entitetima. Poželjno je redovno održavanje postojećih i ostvarivanje novih kontakata sa lokalnim i regionalnim partnerima i klijentima, kao i kreiranje adekvatnih baza podataka. Međutim, tokom sva četiri osnovna procesa dolazi do razmene informacija, zato je važno pažljivo izabrati partnerske organizacije kako bi se očuvao integritet, poverljivost i raspoloživost podataka.

ŠTA RADI POSEBAN CERT?

Pored nacionalnih CERT-ova koji se sveobuhvatno bave bezbednosnim incidentima u IKT sistemima na nacionalnom nivou, širom sveta postoji veliki broj posebnih CERT-ova, fokusiranih na unapređenje informacione bezbednosti u okviru jedne društvene oblasti, grupe subjekata, pa čak i unutar samo jedne kompanije. Recimo, gigant onlajn prodaje Amazon ima svoj tim za bezbednosne incidente (Amazon SIRT) koji je član organizacije FIRST.[10] Imajući u vidu složenost i specifičnost određene zajednice ili grupe subjekata (akademske institucije, banke i slično), odnosno poverljivu prirodu informacija kojima kompanije upravljaju, posebni CERT-ovi sa svojim visoko specijalizovanim stručnjacima svakako su najkompetentnija adresa za zaštitu od sajber incidenata i uspostavljanje preventivnih mera zaštite. Jedan takav primer je ICS CERT (Industrial Control Systems Cyber Emergency Response Team) kompanije "Kasperski labs", poznatog proizvođača anti-virus softvera.[11] ICS CERT je nekomercijalni projekat kompanije i pruža različite usluge zainteresovanim akterima u industriji. Drugim rečima, ICS CERT besplatno deli informacije i ekspertizu sa mrežom partnera iz više oblasti:

- Analiza usklađenosti sa standardima bezbednosti IKT sistema;
- Informisanje o najčešćim propustima proizvoda koji se koriste u industrijskim informacionim sistemima;
- Pružanje informacija o malveru i drugim vrstama pretnji po bezbednost IKT sistema;
- Daljinska detekciju pretnji, tj. procena ljudskog faktora i lanca povezanih aktera (npr. kompanija podizvođača);
- Opšta procena bezbednosti IKT sistema;
- Testiranje otpornosti IKT sistema na napade;
- Analiza malicioznih fajlova;
- Analiza drugih predmeta iz IKT sistema (radnih stanica, mrežnih uređaja, eksternih memorija); - Koordinacija postupaka prilikom napada.[12]

Akademske institucije koje često dele informacionu infrastrukturu, poput Akademske mreže Srbije - AMRES, takođe imaju specifične potrebe u zaštiti informacione bezbednosti. Radi što bolje koordinacije prilikom bezbednosnih incidenata i odgovora na njih, osnivaju se posebni CERT-ovi i za akademske zajednice. Primer takvog posebnog CERT-a jeste ILAN-CERT Istraživačko-akademske

10 Informacije o Amazon SIRT-u dostupne su na: first.org
11 Kaspersky Lab ICS CERT: ics-cert.kaspersky.com
12 Usluge ICS CERT: ics-cert.kaspersky.com

mreže Izraela, koji je član FIRST organizacije od 1995. godine. ILAN-CERT je zadužen za bezbednost mreže više univerziteta širom Izraela.[13]

Centar za bezbednosne incidente (Security Incident Response Center - CAIS) Akademske mreže Brazila osnovan je 1997. godine s ciljem da sačuva bezbednost mreže, otkrije, upravlja i spreči bezbednosne rizike. Do sada, Centar je dokumentovao nekoliko hiljada slučajeva, a među uslugama koje pruža nalaze se i katalog prevara, razvoj akademskih CSIRT-ova na univerzitetima u Brazilu, podizanje svesti i edukacija o informacionoj bezbednosti i rešavanje bezbednosnih incidenata.[14]

KAKO REGISTROVATI POSEBAN CERT U SRBIJI

Delatnosti i poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima može obavljati i organizacija koja nije registrovana kao poseban CERT, ali formalna registracija svakako može poboljšati odnos sa korisnicima kao i saradnju sa drugim CERT-ovima i sličnim organizacijama.

Postupak upisa u evidenciju posebnih CERT-ova, koju vodi Nacionalni CERT, regulisan je Pravilnikom o bližim uslovima za upis u evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima[15] kao i Procedurom za upis u evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima.[16] Ovim aktima propisani su uslovi koje pravno lice ili organizaciona jedinica pravnog lica treba da ispunjava kako bi mogla biti upisana u Evidenciju posebnih CERT-ova:

- da ima sedište na teritoriji Republike Srbije;
- da je pravno lice ili organizaciona jedinica u okviru pravnog lica;
- da obavlja poslove prevencije i zaštite od bezbednosnih rizika u IKT sistemima u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično.

Prijava za upis se podnosi Nacionalnom CERT-u na propisanom obrascu koji je dat u prilogu Pravilnika. U prijavi je potrebno popuniti sledeće podatke o posebnom CERT-u:

- Naziv subjekta (pravnog lica) koji podnosi prijavu;
- Naziv posebnog CERT-a;
- Sedište (mesto, ulica i broj);
- Matični broj;
- Poresko-identifikacioni broj (PIB);
- Broj telefona;
- Broj faksa;
- Adresa internet strane;
- Adresa elektronske pošte.

Prijava treba da sadrži i podatke o odgovornom licu u posebnom CERT-u:

- Ime i prezime;
- Funkcija;
- Broj službenog telefona;
- Službena adresa elektronske pošte.

Uz registracionu prijavu se mora dostaviti i dokaz o obavljanju poslova prevencije i zaštite od bezbednosnih rizika u IKT sistemima. Podnosiocu se ostavlja sloboda da odluči na koji način će dokazivati da obavlja ove poslove, pa tako može podneti

13 ILAN-CERT: first.org
14 CAIS/RNP: rnp.br
15 Ministarstvo trgovine, turizma i telekomunikacija, Pravilnik o bližim uslovima za upis u evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima, 2017. Dostupno na: ratel.rs
16 RATEL, Procedura za upis u evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima, 2017. Dostupno na: ratel.rs

izvod iz statuta ili normativnog akta podnosioca koji uređuje i opisuje obavljanje poslova posebnog CERT-a, izvod iz sistematizacije radnih mesta ili ugovora o radu kojima je za određene zaposlene uvtrđeno obavljanje spomenutih poslova, neki drugi akt pravnog lica ili bilo koja druga dokumentacija kojom podnosilac dokazuje da se bavi obavljanjem ovih poslova.

Prijava se može podneti u pisanom obliku, neposredno u prostorijama Nacionalnog CERT-a ili poštom, a moguće je podneti je i elektronskim putem na internet strani Nacionalnog CERT-a. Ipak, u slučaju da se prijava podnosi elektronskim putem neophodno je u roku od pet dana podneti papirnu dokumentaciju, tj. obrazac i dokaze, osim ukoliko je prilikom podnošenja elektronskim putem ova dokumentacija bila potpisana kvalifikovanim elektronskim potpisom ovlašćenog lica.

Na osnovu podnete prijave i u slučaju da su ispunjeni uslovi propisani Zakonom i Pravilnikom, Nacionalni CERT donosi rešenje kojim se uvrđuje ispunjenost ovih uslova i posebni CERT se upisuje u evidenciju posebnih CERT-ova.

CERT U SVETU

Kao vodeće organizacije za unapređenje standarda informacione bezbednosti, CERT-ovi imaju veliki značaj i za kulturu bezbednosti informacionih sistema. Budući da su u svetu čitavi sistemi javne uprave, obrazovanja, bankarstva, nauke i trgovine, svoje poslovanje najvećim delom preneli u digitalno okruženje, bezbednost postaje vitalno pitanje ne samo ovih sistema, već i samog društva. Stoga, pored nacionalnih CERT-ova koji prate stanje informacione bezbednosti na nivou cele države, postoje i posebni CERT timovi specijalizovani za pojedine oblasti, od čije brzine i efikasnosti često zavisi funkcionalnost sistema, kao i opšti nivo bezbednosne kulture u zajednici. Međunarodna saradnja nacionalnih i posebnih CERT-ova u tome može imati ključni značaj.

Primer je takvog CERT-a je CERT Evropske unije - CERT-EU. Posle jednogodišnjeg pilot programa, institucije Evropske unije su u septembru 2012. odlučile da formiraju Centar za prevenciju bezbednosnih rizika u informacionim sistemima Evropske unije (CERT-EU). Ovaj regionalni CERT čine stručnjaci za informacionu bezbednost iz vodećih institucija EU: Evropske komisije, Generalnog sekretarijata Saveta EU, Evropskog parlamenta, Komiteta regiona i Evropskog ekonomskog i socijalnog komiteta. CERT-EU aktivno sarađuje sa CERT-ovima država članica EU, kao i sa kompanijama čija je primarna delatnost informaciona bezbednost.[17]

17 CERT-EU: cert.europa.eu

MEĐUNARODNE ORGANIZACIJE

MEĐUNARODNE ORGANIZACIJE

TRUSTED INTRODUCER

Sistem "Trusted Introducer" ustanovila je evropska CERT zajednica 2000. godine u cilju izgradnje servisne infrastrukture i pružanja specifičnih usluga samim CERT-ovima.[18] Ovaj servis je istovremeno svojevrsni klirinški zavod koji garantuje ispunjenje obaveza, ažurira informacije i posreduje u komunikaciji. Servis ima oko 300 upisanih članica iz zemalja Evrope i sveta, uz dvostepenu kategorizaciju dodatnih usluga za akreditovane i seritifkovane timove. Deo usluga dostupan je i široj javnosti kroz pretragu direktorijuma članica, njihovih podataka i kontakata.[19] Status akreditovanog, odnosno sertifkovanog tima stiče se na osnovu utvrđene procedure, uz godišnju nadoknadu.

U "Trusted Introducer" direktorijumu timovi iz Srbije imaju status kako izlistanih, tako i akreditovanih članova i to:

- CSIRT Akademske mreže Srbije koji je 2011. godine izlistan;
- CERT Ministarstva unutrašnjih poslova koji je 2016. godine izlistan a akreditovan 2018. godine;
- Share CERT koji je 2017. godine izlistan a akreditovan 2018. godine;
- Nacionalni CERT koji je 2017. godine izlistan a akreditovan 2019. godine i
- UNICOM CERT koji je 2019. godine izlistan.

FIRST

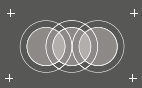
Od nastanka Foruma timova za odgovor na incidente i bezbednost (Forum of Incident Response and Security Teams, FIRST) 1990. godine, njegovi članovi se bave rešavanjem neprekidnog niza pretnji i napada na računarske mreže i sisteme povezane preko interneta. Forumu je pristupio širok spektar timova koji se bave bezbednosnim pretnjama, uključujući timove iz komercijalnog, akademskog i državnog sektora.[20]

FIRST okuplja preko 500 timova iz više od 90 različitih država, u statusu punopravnih ili pridruženih članova.[21] Punopravno članstvo podrazumeva pravo glasanja i predlaganja novih pridruženih i punopravnih članova. Nacionalni CERT Republike Srbije je početkom 2019. godine zahvaljujući First Fellowship programu postao deo FIRST (Forum of Incident and Response Security Teams) organizacije i time dobio mogućnost da po prvi put učestvuje na godišnjoj FIRST konferenciji posvećenoj informacionoj bezbednosti. Prisustvom na ovoj konferenciji, Nacionalni CERT Republike Srbije otpočeo je proceduru za dobijanje statusa punopravnog člana u organizaciji FIRST.

18 Trusted Introducer: trusted-introducer.org
19 Direktorijum TI: trusted-introducer.org
20 O FIRST-u: first.org
21 Mapa FIRST članova: first.org

ITU

Međunarodna telekomunikaciona unija (ITU), specijalizovana agencija pri Ujedinjenim nacijama, bavi se komunikacionim i informacionim tehnologijama. U okviru posebnog CIRT programa, ITU sarađuje sa državama članicama UN, kao i regionalnim organizacijama, na izgradnji kapaciteta za koordinisane odgovore na sajber napade. Takođe, ITU pruža podršku u procesu planiranja, implementacije i operativnosti nacionalnih CERT-ova. U okviru ovog programa, ITU sprovodi procenu spremnosti država za uspostavljanje nacionalnih timova koja je, između ostalih, sprovedena i u državama regiona, i to u Crnoj Gori, Albaniji, Makedoniji i Srbiji. ITU mrežu čine 109 nacionalnih CERT-ova.[22]


2019